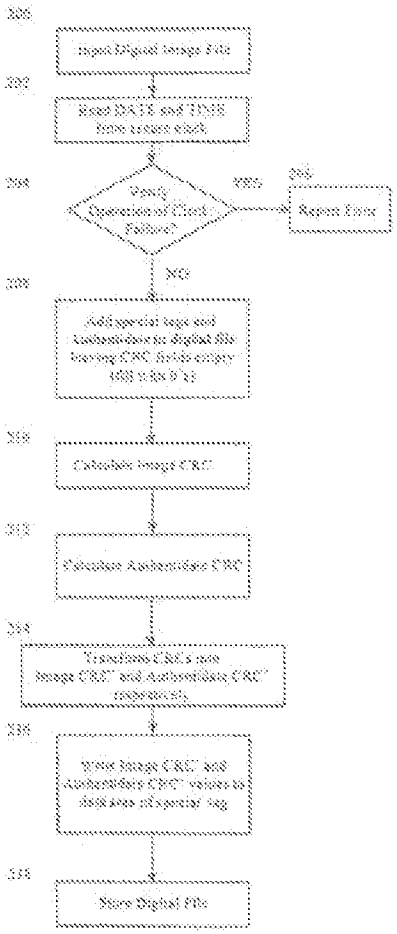
DIGITAL FILE MANAGEMENT AND IMAGING SYSTEM AND METHOD INCLUDING SECURE FILE MARKING

Publication number: JP2002538536 (T)
Publication date: 2002-11-12
Inventor(s):
Applicant(s):
Classification:
- international: ***H04L9/32;*** **H04L9/32;** (IPC1-7): G06F12/14; G06F11/10; G06F12/00; G06T1/00; H04N1/40
- European: H04L9/32; H04L9/32T
Application number: JP20000601785T 20000224
Priority number(s): US19990259135 19990226; WO2000US05098 20000224

Also published as:
WO0051286 (A1)
US2004049521 (A1)
US7415476 (B2)
EP1159799 (A1)
EP1159799 (B1)
more >>

Abstract not available for JP 2002538536 (T)
Abstract of corresponding document: **WO 0051286 (A1)**

A digital file management and imaging system records additional independent data with each stored image (200) including a true date gleaned from a secure clock (202) not settable by a user, a number derived from a cyclic redundancy code (CRC) algorithm for the image data (210) and the true date (212). This additional data is recorded within each digital file as soon as possible after the file is acquired. If the file is altered in any way after the recording of the additional data, recalculation of the image CRC on the altered file will not match the original image CRC recorded within it. Thus, the fact that it has been altered can be detected. Likewise, if the true date is altered in any way, recalculation of the date CRC will similarly reveal this fact.



(19)日本国特許庁（ＪＰ）　(12)**公表特許公報（Ａ）**　(11)特許出願公表番号
特表2002－538536
（P2002－538536A）
(43)公表日　平成14年11月12日(2002.11.12)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ	５Ｂ００１
	11/10	３３０	11/10	３３０Ａ	５Ｂ０１７
	12/00	５２０	12/00	５２０Ｅ	５Ｂ０５０
		５３７		５３７Ｚ	５Ｂ０８２
Ｇ０６Ｔ	1/00	２００	Ｇ０６Ｔ　1/00	２００Ａ	５Ｃ０７７

審査請求　未請求　予備審査請求　有　（全 38 頁）　最終頁に続く

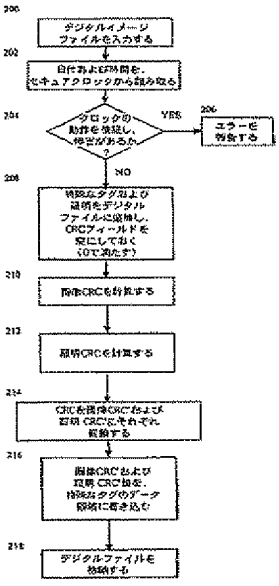
(21)出願番号　特願2000－601785(P2000－601785)
(86)(22)出願日　平成12年２月24日(2000.2.24)
(85)翻訳文提出日　平成13年８月27日(2001.8.27)
(86)国際出願番号　ＰＣＴ／ＵＳ００／０５０９８
(87)国際公開番号　ＷＯ００／５１２８６
(87)国際公開日　平成12年８月31日(2000.8.31)
(31)優先権主張番号　０９／２５９，１３５
(32)優先日　平成11年２月26日(1999.2.26)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　オーセンティデイト　ホールディング　コーポレイション
アメリカ合衆国　12308　ニューヨーク州　スケネクタディー　リバーサイド　テクノロジー　パーク　テクノロジー　ドライブ　2165
(72)発明者　コリン　ディー．ボローマン
アメリカ合衆国　12303　ニューヨーク州　スケネクタディー　マーサー　アベニュー　112
(74)代理人　弁理士　谷　義一　（外２名）

最終頁に続く

(54)【発明の名称】　確実なファイルマークキングを含む、デジタルファイル管理およびイメージングシステムおよび方法

(57)【要約】
デジタルファイル管理およびイメージングシステムは、格納された各画像に、追加の独立データを記録し、格納された各画像（２００）は、セキュアクロックから収集され、ユーザによって設定可能でない真の日付（２０２）を含み、画像データ（２１０）および真の日付（２１２）について、巡回冗長コード（ＣＲＣ）アルゴリズムから導出された数を含む。この追加のデータは、ファイルが獲得された後、可能な限りすぐに各デジタルファイル内に記録される。ファイルが、追加のデータの記録後にいずれかの方法において改変された場合、改変されたファイルにおける画像ＣＲＣの再計算が、その内部に記録された元の画像ＣＲＣと合致しない。したがって、これが改変されたという事実を検出することができる。同様に、真の日付がいずれかの方法において改変された場合、日付ＣＲＣの再計算が、類似の方法でこの事実を明かす。



【特許請求の範囲】

【請求項１】　デジタルファイルを入力する手段と、

日付および時間情報を提供する確実な日付および時間基準と、

前記日付および時間情報から導出された日付／時間値を生成する手段と、

前記デジタルファイルから導出された画像値を生成する手段と、

前記デジタルファイルに、前記日付および時間情報、前記日付／時間値、および前記画像値をマーキングする手段と、

前記マーキングされたデジタルファイルを格納する手段と

を備えたことを特徴とするデジタルファイル管理およびイメージングシステム。

【請求項２】　前記確実な日付および時間基準は、ローカルのセキュアクロックであることを特徴とする請求項１に記載のシステム。

【請求項３】　前記日付および時間値を生成する手段は、巡回冗長コードアルゴリズムを実行することを特徴とする請求項１に記載のシステム。

【請求項４】　前記画像値を生成する手段は、巡回冗長コードアルゴリズムを実行することを特徴とする請求項１に記載のシステム。

【請求項５】　前記日付／時間値を変換する手段をさらに含み、前記マーキングする手段は、前記デジタルファイルに、前記変換された日付／時間値をマーキングすることを特徴とする請求項１に記載のシステム。

【請求項６】　前記日付／時間値を変換する手段は、数学的変換を実行することを特徴とする請求項５に記載のシステム。

【請求項７】　前記画像値を変換する手段をさらに含み、前記マーキングする手段は、前記デジタルファイルに、前記変換された画像値をマーキングすることを特徴とする請求項１に記載のシステム。

【請求項８】　前記画像値を変換する手段は、数学的変換を実行することを特徴とする請求項７に記載のシステム。

【請求項９】　前記デジタルファイルは、画像ファイルであることを特徴とする請求項１に記載のシステム。

【請求項１０】　前記デジタルファイルは、テキストファイルであることを

特徴とする請求項１に記載のシステム。

【請求項１１】　前記デジタルファイルは、デジタルカメラからのファイルであることを特徴とする請求項１に記載のシステム。

【請求項１２】　前記デジタルファイルは、医療画像デバイスからのものであることを特徴とする請求項１に記載のシステム。

【請求項１３】　前記デジタルファイルは、コンピュータアプリケーションにより生成されたファイルであることを特徴とする請求項１に記載のシステム。

【請求項１４】　マーキングされたファイルを検証する手段をさらに含むことを特徴とする請求項１に記載のシステム。

【請求項１５】　デジタルファイルと、

日付および時間情報を提供する確実な日付および時間基準と、

前記日付および時間情報から導出された日付／時間値と、

前記デジタルファイルから導出された画像値と、

前記日付および時間情報、前記日付／時間値、および前記画像値をマーキングされた、マーキングされたデジタルファイルと

を備えたことを特徴とするデジタルファイル管理システム。

【請求項１６】　前記確実な日付および時間基準は、ローカルのセキュアクロックであることを特徴とする請求項１５に記載のシステム。

【請求項１７】　前記日付および時間値は、巡回冗長コードアルゴリズムによって導出されることを特徴とする請求項１５に記載のシステム。

【請求項１８】　前記画像値は、巡回冗長コードアルゴリズムによって導出されることを特徴とする請求項１５に記載のシステム。

【請求項１９】　変換された日付／時間値をさらに含み、前記マーキングされたファイルは、前記変換された日付／時間値をマーキングされることを特徴とする請求項１５に記載のシステム。

【請求項２０】　変換された画像値をさらに含み、前記マーキングされたファイルは、前記変換された画像値をマーキングされることを特徴とする請求項１５に記載のシステム。

【請求項２１】　前記デジタルファイルは、画像ファイルであることを特徴

とする請求項１５に記載のシステム。

【請求項２２】　前記デジタルファイルは、テキストファイルであることを特徴とする請求項１５に記載のシステム。

【請求項２３】　前記デジタルファイルは、デジタルカメラからのファイルであることを特徴とする請求項１５に記載のシステム。

【請求項２４】　前記デジタルファイルは、医療画像デバイスからのものであることを特徴とする請求項１５に記載のシステム。

【請求項２５】　前記デジタルファイルは、コンピュータアプリケーションにより生成されたファイルであることを特徴とする請求項１５に記載のシステム。

【請求項２６】　デジタルファイルを提供するステップと、

ローカルソースからの確実な日付および時間基準から日付および時間情報を提供するステップと、

前記日付および時間基準から導出された日付／時間値を生成するステップと、

前記デジタルファイルから導出された画像値を生成するステップと、

前記デジタルファイルに、前記日付および時間情報、前記日付／時間値、および前記画像値をマーキングするステップと、

前記マーキングされたデジタルファイルを格納するステップと

を備えたことを特徴とするデジタルファイル管理およびイメージングの方法。

【請求項２７】　前記日付および時間値を生成するステップは、巡回冗長コードアルゴリズムを実行することを特徴とする請求項２６に記載の方法。

【請求項２８】　前記画像値を生成する手段は、巡回冗長コードアルゴリズムを実行することを特徴とする請求項２６に記載の方法。

【請求項２９】　前記日付および時間値を変換し、前記デジタルファイルに、前記変換された日付および時間値をマーキングするステップをさらに含むことを特徴とする請求項２６に記載の方法。

【請求項３０】　前記画像値を変換し、前記デジタルファイルに、前記変換された日付および時間値をマーキングするステップをさらに含むことを特徴とする請求項２６に記載の方法。

【請求項３１】　前記デジタルファイルを提供するステップは、元の画像をデジタルイメージに光学式走査することを含むことを特徴とする請求項２６に記載の方法。

【請求項３２】　前記日付／時間値および画像値を再計算すること、および、前記再計算された値を、それぞれ前記画像においてマーキングされた前記日付／時間および画像値と比較することをさらに含むことを特徴とする請求項２６に記載の方法。

【発明の詳細な説明】

【０００１】

（発明の分野）

本発明は、一般にデジタルイメージングシステムに関し、より詳細にはデジタルファイル認証に関する。

【０００２】

（発明の背景）

デジタルイメージングは、画像またはオブジェクトをデジタルラスタイメージとして表現および格納することである。デジタルイメージングは、ますます多数の産業において使用されており、これは部分的には、使用可能にする技術の向上した可用性のためであり、部分的には、従来の格納方法に勝るように提供された多数の利点によるものであり、これには、低減された記憶空間、向上されたアクセス速度、集中された検索可能性（たとえば、探索機能）、文書の「複数」かつ「バックアップ」コピーを好都合に作成する能力、および、文書を高速に転送あるいは伝送する能力が含まれる。

【０００３】

紙の文書が原本である場合、デジタルイメージングシステムは、典型的に、紙の文書を走査し、走査された文書の表現をデジタルラスタイメージとして格納する。光学式走査デバイスは、典型的に、紙の原本の画像を、デジタルイメージとして格納するために走査するように使用される。走査された画像は、原本の厳密な表現であり（走査デバイスの解像度の制限によってのみ制限される）、手書き、署名、写真、図などを含むことができる。別法として、デジタルカメラ、医療画像デバイス、または他のソースから生じるデジタルイメージも、デジタルイメージングシステムに格納することができる。

【０００４】

既知のイメージング技術の１つの欠点は、たとえば、詐欺行為をするために改変される、デジタルイメージの固有の能力である。たとえば、原本の紙の文書を不正に変更することができ、このような不正な変更（消去または追加）は、典型的に、隠そうとしても自然に現れる証拠を残すが、他方、これらの文書のデジタ

ルイメージは、このような証拠を残さずに完全に改変することができる。したがって、画像の真実性が重要であり、問題となる可能性がある場合（たとえば、法的および医療の分野）、デジタルイメージの使用はしばしば好ましくなく、受け入れ可能でなく、認容可能でなく、したがってしばしば回避される。

【０００５】

多数の異なるデジタル画像フォーマットが使用可能であるが、各場合において、データが潜在的に改変可能である。デジタルイメージングシステムが明示的に編集機能を提供しない場合でも、画像をサードパーティのツールにより編集することができる。

【０００６】

提案された解決策は、追記型（「ＷＯＲＭ」）光媒体を使用してデジタルイメージを格納することである。ＷＯＲＭ媒体格納の１つの利点は、それが収容するデータが本質的に改変不可能であり、データをただ一度だけ媒体に書き込むことができることである。しかし、この手法には、いくつかの欠点もある。たとえば、ＷＯＲＭ媒体上に記録されたデータを、元の記録のＷＯＲＭディスクから書き換え可能媒体へコピーし、改変し、次に、このようなイベントの追跡可能性なしに、新しいＷＯＲＭディスク上へ記録することができる。

【０００７】

加えて、大きな信頼と共に、いかなる１つの特定のＷＯＲＭディスク上のデータも、それがそのディスク上で記録されたので改変されていないと述べることはできるが、データが記録された日付および時間、または、データがいかなる種類の「原本」と合致するかどうかは、あらゆるまたは限定的な手段によっても決定することができない。

【０００８】

ファイル検証技術において知られている進歩は、デジタルファイル（画像、ワードプロセッサ文書、オーディオまたはビデオクリップなど）の「電子署名」の登録に提供される。ユーザがローカルでファイルを選択し、サービスプロバイダによって提供されたプログラムをローカルで作動させ、ファイル内容にのみ基づいた、選択されたデジタルファイルの「電子署名」を作成できることが知られて

いる。署名は、ユーザにより提供されたファイル名およびユーザにより選択されたキーワードと共に、プロバイダのサイトにアップロードされ、サービスプロバイダによって保守された登録データベースに、特定のユーザ用に確立されたアカウント下で格納される。１つの特定のプロバイダが「登録証明書」を生成し、これはとりわけ署名を示す。

【０００９】

デジタルファイルの内容および提出日を後で検証するには、オンラインでサービスプロバイダのサイトにアクセスし、以前の登録レコードをファイル名またはキーワードによって検索することが必要である。検索されたデータベースレコードが、ファイル署名、および、ファイル署名が登録された元の日付を示す。検証を完了するには、ユーザが電子署名プログラムを、検証されるファイル上で作動（再度ローカルで）させなければならず、再生成された署名を、検索された登録済み署名と比較して、問題のデジタルファイルの署名が、元の登録されたファイルのものに合致するかどうかを決定しなければならない。

【００１０】

このとき、ユーザが有するものは、所有しているファイルの署名が、特定の日に登録されたファイルの署名と合致するという検証である。

【００１１】

（発明の概要および目的）

既知のデジタルイメージングシステムにおける画像認証における、前述および他の問題および欠陥が、本発明によって解決され、確実な（ｓｅｃｕｒｅ）画像マークキングによるデジタルファイル認証を提供するための技術的進歩が、本発明によって達成される。

【００１２】

様々な態様において、本発明の目的は、確実なファイルマークキングによるデジタルファイル認証を提供するデジタルファイル管理のためのシステムおよび方法を提供することである。

【００１３】

本発明の一実施形態におけるデジタルファイル管理システムは、デジタルファ

イルを入力するための手段、および、日付および時間情報を提供する確実な日付および時間基準を含む。日付／時間値が生成され、これは確実な日付および時間情報から導出される。画像値が、デジタルファイル自体から導出される。デジタルファイルが、日付および時間情報、日付／時間値、および画像値によりマークキングされる。次いで、マークキングされたデジタルファイルが格納される。

【００１４】

代替実施形態は、日付／時間値および画像値を巡回冗長コードアルゴリズムによって生成すること、および、日付／時間値および画像値を、数学的変換を介して変換すること、およびデジタルファイルに、変換された値によりマークキングすることなどの機能を含むことができる。

【００１５】

他の実施形態では、確実な日付および時間基準が、ローカルのセキュアクロック（ａ　ｓｅｃｕｒｅ　ｃｌｏｃｋ）である。

【００１６】

様々な実施形態では、デジタルファイルを画像ファイル、テキストファイルまたは他のいかなるファイルフォーマットにすることもできる。

【００１７】

本発明の代替実施形態は、元の画像をデジタルイメージに走査するための光学式スキャナ、あるいは、直接デジタルカメラまたは医療画像装置からの、デジタルイメージの入力を可能にする。マーキングされたデジタルファイルを、光学記憶装置に格納することもできる。

【００１８】

（図面の詳細な説明）

本発明の以下の記載は、例示のために、ターンキー文書管理およびイメージングシステム、ＤｏｃＳＴＡＲ（商標）に組み込まれたＡｕｔｈｅｎｔｉｄａｔｅ（商標）画像認証システムを使用し、これらは共に、本発明の譲受人であるＢｉｔＷｉｓｅ　Ｄｅｓｉｇｎｓ，Ｉｎｃから入手可能である。本発明のＤｏｃＳＴＡＲ実施形態は、紙の文書の原本を格納し、マーキングし、認証することに適応されるが、以下に記載されるように、いかなるデジタルファイルも、本発明の方

法およびシステムによって処理することができる。ＤｏｃＳＴＡＲ実施形態を参照した以下の考察は、決して限定となるように意図されるものではなく、本発明の説明および理解を容易にするための、例示のためのものにすぎない。

【００１９】

図１は、本発明を実装したＤｏｃＳＴＡＲ文書管理およびイメージングシステムの実施形態を示す。

【００２０】

ＤｏｃＳＴＡＲシステムホスト１００は、入力デバイス１１０、記憶デバイス１２０および確実な時間および日付基準１３０と通信するように構成されている。

【００２１】

この実施形態において、システムホスト１００は、ＩＢＭ　ＰＣまたはワークステーションとして実装され、入力デバイス１１０は光学式スキャナであり、記憶デバイス１２０は光学記憶デバイスであり、確実な時間および日付基準１３０は、セキュアクロックを組み込むハードウェアキーによって提供される。

【００２２】

元の画像が、光学式スキャナ１１０によって走査される。本発明の方法によれば、結果として生じるデジタルイメージが、システムホスト１００によって処理され、これは本明細書で以下に詳細に論じられ、次に、光学記憶デバイス１２０上に格納され、ここから後に検索することができる。

【００２３】

本発明の画像認証システムは、一態様において、追加の独立データを、格納された各デジタルファイルに記録することによって動作する。これらの追加のデータは、セキュアクロックから収集される（以下でさらに詳細に記載される）「真の日付」を含み、これはユーザによって設定可能ではなく（Ａｕｔｈｅｎｔｉｄａｔｅ（商標））、画像データに対して巡回冗長コード（ＣＲＣ）アルゴリズム（以下でさらに詳細に記載される）から導出された数を含み、この数は、「画像ＣＲＣ」と呼ばれ、さらに、「真の日付」から導出されたＣＲＣを含み、これが「日付ＣＲＣ」と呼ばれる。

【００２４】

これらの追加のデータは、画像がシステムによって（たとえば、ＤｏｃＳＴＡＲ実施形態におけるスキャナ１１０から）獲得された後に、可能な限りすぐに、各デジタルファイル内に記録されることが好ましい。以下でさらに詳細に論じられるように、画像が、追加のデータの記録後にいずれかの方法において改変された場合に、改変された画像における画像ＣＲＣの再計算が、その内部に記録された元の画像ＣＲＣと合致しない。したがって、画像が改変されたか、あるいはそうでない場合は、損なわれたという事実を、検出することができる。同様に、真の日付がいずれかの方法において改変された場合、日付ＣＲＣの再計算が、類似の方法でこの事実を明かす。

【００２５】

画像および日付ＣＲＣを、いかなるときも検査かつ検証することができる。再計算された値が、記録された値に合致した場合、厳密な信頼と共に、現在記録されている画像が、指定された日付に記録されており、そのとき以来いかなる方法においても改変されていないと述べることができる。紙の格納を含む、他の既知のシステムは、文書の作成日または真正に関して類似の保証を提供することができない。

【００２６】

図２を参照して、本発明の動作を開示する。

【００２７】

デジタルファイルが最初に獲得される（記憶装置から検索されるか、あるいは、入力デバイス１１０から受信される）。（ステップ２００）。日付および時間情報が、セキュアクロック１３０から得られる（ステップ２０２）。セキュアクロックの適切な動作が査定される（ステップ２０４）。セキュアクロックが機能しているとみなされた場合、日付および時間データが、クロックからの読み取りとして受け入れられる（ステップ２０２）。セキュアクロックの障害が判定された場合、エラー指示が返され、画像処理が中止される（ステップ２０６）。クロックが機能しているとみなされると（ステップ２０４）、（以下に論じられるような）特殊なタグおよび証明情報（ｔｈｅ　Ａｕｔｈｅｎｔｉｄａｔｅ　ｉｎｆ

ｏｒｍａｔｉｏｎ）（日付および時間を含む）がデジタルファイルに追加され、ＣＲＣデータフィールドが０に初期化される（すなわち、データフィールドが０で満たされる）（ステップ２０８）。

【００２８】

次いで、２つの算出値が計算され、これらが画像コンテンツおよび証明情報からそれぞれ導出される。算出値は、いかなる様式においても、デジタルファイル内に含まれたデータに基づいて計算することができ、これによりデータの汚染の検出、たとえば、標準のチェックサムなどが可能となる。本発明のこの実施形態では、巡回冗長コード（「ＣＲＣ」）という、本質的により複雑なチェックサム計算が使用されて、算出値が導出される。しかし、いかなる計算方法も受け入れ可能であり、これにより、文書コンテンツデータから導出され、データの汚染の検出に適した数値を提供する。

【００２９】

この実施形態では、算出値が、既知のＣＲＣアルゴリズム（以下でさらに詳細に論じられる）によって生成され、これは、画像コンテンツおよび証明（ｔｈｅ Ａｕｔｈｅｎｔｉｄａｔｅ）において動作され、画像ＣＲＣおよび証明ＣＲＣがそれぞれ作成される（ステップ２１０、２１２）。画像ＣＲＣおよび証明ＣＲＣが、専有の（（ｐｒｏｐｒｉｅｔａｒｙ）数学的変換によって追加のセキュリティのために「変換」され（以下で論じられるように）、画像ＣＲＣ′および証明ＣＲＣ′が作成される（ステップ２１４）。

【００３０】

次に、画像ファイルは、画像ＣＲＣ′および証明ＣＲＣ′によりマーキングされる（ステップ２１６）。マーキングされたデジタルファイルが光媒体上に、光学記憶デバイス１２０によって格納される（ステップ２１８）。

【００３１】

次に、画像および時間と日付スタンプの真正を、デジタルファイル内に格納された算出値を検査することによって、続いて判定することができ、これは、ファイルされた画像のＣＲＣを検証するための一実施形態を記載する例示的流れ図を示す図３に示したように行われる。

【００３２】

デジタルファイルにおいてＣＲＣを検証することの最初のステップは、特殊なタグおよび日付領域を読み取り、格納された画像ＣＲＣおよび日付ＣＲＣ値を検索することである（ステップ３００）。ＣＲＣ値がデジタルファイルにおいて位置付けることができないか、あるいは読み取ることができなかった場合（ステップ３０２）、画像が適切にファイルされていないか、あるいは、画像が改変されたか、あるいはそうでない場合は損なわれていると決定され、エラーが通知される（ステップ３０４）。特殊なタグが発見された場合、ＣＲＣが、デジタルファイルおよび日付文字列について再計算される（ステップ３０６）。ＣＲＣを最初に計算するために使用されたものと同じアルゴリズムが使用されて、この時点でこれらが再生成される。再計算された画像ＣＲＣが変換され、タグから読み取られた画像ＣＲＣと比較される（ステップ３０８）。（別法として、格納された画像ＣＲＣを、再計算された値との比較の前に、逆変換することができる）。再計算されたデジタルファイルＣＲＣが、特殊なタグに格納されたものと合致しなかった場合、画像が改変されたか、あるいはそうでない場合は汚染されたと決定され、エラーが指示される（ステップ３１０）。格納された画像ＣＲＣおよび再計算された画像ＣＲＣが好ましく比較されると（すなわち、これらが合致した）、日付ＣＲＣがテストされる。再計算された日付ＣＲＣが変換され、タグから読み取られた日付ＣＲＣと比較される（ステップ３１２）。（別法として、格納された日付ＣＲＣを、再計算された値との比較の前に、逆変換することができる）。再計算された日付ファイルＣＲＣが、特殊なタグに格納されたものと合致しなかった場合、日付文字列が改変されたか、あるいはそうでない場合は汚染されたと決定され、エラーが指示される（ステップ３１４）。日付ＣＲＣが合致し、この時点で、画像および日付ＣＲＣが好ましく比較されると、デジタルファイルが改変されていないと決定され、故に証明される（ステップ３１６）。

【００３３】

前述の記載から理解されるように、確実な、信用を損なわないクロックの使用が、本発明に必須である。これは、ユーザによって改変することができない確実な時間および日付ソースとしての機能を果たす。セキュアクロックは、コンピュ

ータの電源がオフにされたときでも、バッテリのバックアップを用いて、時間および日付を維持する。

【００３４】

セキュアクロックを提供する、カスタム設計されたハードウェアまたは市販の製品を使用することができる。いずれの場合も、機構は、不正あるいは恣意的な日付／時間調整を適切に防止しなければならない。

【００３５】

ＤｏｃＳＴＡＲ実施形態では、セキュアクロックを物理的なハードウェアキーに組み込む市販の製品が利用される（時として、「ドングル（ｄｏｎｇｌｅ）」と呼ばれる）。ハードウェアキーが、コンピュータのパラレルポートに接続し、メーカによって提供されたアプリケーションプログラミングインターフェイス（ＡＰＩ）を介してアクセスすることができる。

【００３６】

本発明のＤｏｃＳＴＡＲ実施形態の使用で選択されたハードウェアキーは、ＴＩＭＥＨＡＳＰ－４であり、Ａｌａｄｄｉｎ Ｋｎｏｗｌｅｄｇｅ Ｓｙｓｔｅｍｓ，ＬＴＤ．から入手可能である。ハードウェアキーのセキュリティは、カスタムのＡＳＩＣチップ（特定用途向けＩＣ）、システムプロバイダ（たとえば、本願の譲受人でありＤｏｃＳＴＡＲシステムの「プロバイダ」であるＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．）によってのみ使用される一意の組のパスワード、および、メーカのプログラミングインターフェイスおよびデバイスドライバにおける高度の保護アルゴリズムおよびアンチデバッギング技術によって保護される。これは、セキュアクロックのために高度のセキュリティを提供する。

【００３７】

現在の日付および時間は、ＤｏｃＳＴＡＲホストコンピュータの組立中に、ハードウェアキー内に含まれたセキュアクロックに、工場内でプログラムされる。いかなる時間設定を使用することもできるが、この実施形態におけるセキュアクロックは、グリニッジ平均時（ＧＭＴ）に設定され、異なる地方時間帯に合わせて、あるいは、夏時間に合わせてクロックを調整する必要性がなくなる。

【００３８】

クロックの調整を行う機構を組み込み、クロックを、経時的に生じる可能性のあるわずかな誤差についてリセットあるいは補正することができる。たとえば、図４に示されたような一実施形態では、セキュアクロックにおける日付および時間を、ユーザのシステム上に常駐する特殊な管理プログラムによって変更することができ、これは、ユーザが、たとえば、本願の譲受人であるＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．のテクニカルサポート部門など、システムプロバイダによって供給された適切な認証コードを供給したときにのみ、確実な日付および時間への変更を許可する。認証コードは、セキュアクロックの日付および時間を、その現在の日付および時間値から、システムプロバイダによって維持された現在のＧＭＴに変更するためにのみ動作する。これは、ユーザがセキュアクロックを恣意的に改変することを防止し、それにより、画像に、不正確あるいは不正な日付および時間をスタンプすることを防止する。

【００３９】

この実施形態では、認証コードが、セキュアクロックを変更するために必要とされる。このコードを得るには、システムプロバイダのシステムにおけるサポート技術者が、ハードウェアキーの通し番号、および、現在のセキュアクロックの日付を、ＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．で維持された保護カスタムプログラム（「Ｅａｇｌｅ Ｃａｌｌ Ｔｒａｃｋｉｎｇ Ｓｙｓｔｅｍ」）に入力し（ステップ４００）、これが認証コードを生成する（ステップ４０２）。認証コードにより、現場の技術者またはエンドユーザが、セキュアクロックを、ＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．で確立され維持された日付および時間にのみ変更することができる。

【００４０】

この実施形態における認証コードは、数学的アルゴリズムを介して決定され、これが、現在のセキュアクロック日付、ハードウェアキーの通し番号、および、日付および時間への所望の変更が与えられると、１つの一意のコードを生じる。この認証コードは、妥当性が制限されており、将来の別の日において、クロックを、認証コードが与えられた日の日付および時間にリセットするように動作しない。

【００４１】

コードがユーザエンドで入力される（ステップ４０４）。所望のクロック設定が、ユーザエンドで入力される（ステップ４０６）。クライアントシステムで使用された管理プログラムが、小さな時間ウィンドウ（２０分）を許容し、これについて入力されたいかなる時間も認証コードに合致する。認証コードは、内部で、与えられた変更の時間の前５分および後１５分の時間について計算される。所与の認証コードが、時間ウィンドウ内のコードのいずれかに合致した場合、認証コードが正しいとみなされ、実施される。これにより、現場の技術者が、認証コードが通知される間に、数分の遅延を補償することができる。

【００４２】

したがって、所望の設定が認証コードに対して検証されて、コードが、要求された日付および時間変更を認証するかどうか決定される（ステップ４０８）。無効が決定された場合、エラーが返され、クロックは更新されない（ステップ４０９）。有効な要求であれば、セキュアクロックへの実際の変更は、Ｕｐｄａｔｅ Ｃｌｏｃｋコマンドがユーザエンドに入力されるまで（ステップ４１０）起こらない。これにより、現場の技術者が、現場のクロックを、ＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．で維持されたクロックと正確に同期化させることができる。Ｕｐｄａｔｅコマンドが発行された後、認証コードがクロック情報に対して再検証されて、それがなお有効であることが保証される（ステップ４１２）。無効が決定された場合、エラーが返され、クロックは更新されない（ステップ４１３）。クロックは更新される（ステップ４１４）。

【００４３】

別法として、セキュアクロックを、サービスプロバイダによって、プロバイダの施設（たとえば、ＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．）で再プログラムすることができ、これは、ハードウェアキーを、ＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．で指定されたＥａｇｌｅシステムに直接接続し、ｕｐｄａｔｅ ｓｅｃｕｒｅ ｃｌｏｃｋコマンドを発行することによる。ハードウェアキーの通し番号が検証され、セキュアクロックの日付および時間が、ＢｉｔＷｉｓｅ Ｄｅｓｉｇｎｓ，Ｉｎｃ．で維持されたＧＭＴの日付および時間に更新される。

【００４４】

さらなる代替実施形態では、経時的に生じる可能性のある誤差について補正するか、あるいはクロックを設定するためのクロック調整を、自動化処理として実装することができ、ユーザがクロック更新を、リモートのセキュアクロックから引き起こすことができるが、ユーザ自身が実際にクロック情報を設定することはできない。

【００４５】

上述したクロック設定および更新の手動または自動の方法が、ユーザがセキュアクロックを恣意的に改変することを防止し、それにより、画像に、不正確あるいは不正な日付および時間をスタンプすることを防止する。

【００４６】

現在使用可能な技術の制限内で予想できるように、各クロックにおけるバッテリが結局は故障し、あるいはそうでない場合は、クロックが経時的に欠陥を有するようになる可能性がある。これらの状態が、ソフトウェアによって、画像処理の前にテストされて、欠陥のあるクロック（または、電気のなくなったバッテリ）から無効な日付が画像に記録されず、したがって、画像マーキングの信頼性が損なわれないことが保証される。クロック障害の場合、画像ファイリングが、クロックが修理あるいは交換されるまで、使用禁止にされる。

【００４７】

図２を参照して言及された、本発明のＤｏｃＳＴＡＲ実施形態における算出値は、巡回冗長コード（ＣＲＣ）である。ＣＲＣは、３２ビットの整数値であり、既知のＣＲＣ－３２アルゴリズムをデータのブロックにおいて実行した結果を表す。ＣＲＣ－３２アルゴリズムは、共通のパブリックドメインアルゴリズムであり、様々な応用例におけるデータの微細な変更を検出するためのものである。たとえば、ＣＲＣが通信分野において使用されて、データが、未知の品質の伝送回線を介して正しく伝送されたことが検証される。これは、普及しているＰＫＺＩＰユーティリティなどにおいて、圧縮されたデータの汚染を検出するためにも使用される。ＣＲＣの強みの１つが、データへの変更を検出することであり、他方、検出されない可能性もある。たとえば、ビットエラーが所与のデータのブロッ

クにおいて起こったが、それらの合計が同時的に元のデータのものと同じであった場合、このエラーは、標準のチェックサムが使用された場合、検出されないままとなる可能性がある。ＣＲＣ－３２アルゴリズムは、このタイプの変更を検出し、これは、結果として生じるコードが、標準チェックサムにおけるように、単に構成要素データの合計ではないからである。

【００４８】

ＣＲＣ－３２アルゴリズムの技術的考察は、本明細書では提示されない。ＣＲＣ－３２アルゴリズムの多数のソースおよびソースコードが、パブリックドメインにある。本発明のＤｏｃＳＴＡＲ実施形態において実施されるＣＲＣ３２アルゴリズムのサンプルＣ＋＋ソースコードを以下に示す。以前に述べたように、ＣＲＣの使用は、本発明のために本質的には必要とされず、画像データから導出されてデータの汚染の検出に適した数値を提供する、いかなる計算方法も受け入れ可能である。例示的Ｃ＋＋ソースコードがここに示される。

【００４９】

【表１】

Sample C++ Source Code to Calculate CRC-32

```
long  CRCTable[] =
      {
       0x00000000L,    0x77073096L,    0x0EE0E612CL,   0x990951BAL,
       0x076DC419L,    0x706AF48FL,    0x0E963A535L,   0x9E6495A3L,
       0x0EDB8832L,    0x79DCB8A4L,    0x0E0D5E91EL,   0x97D2D988L,
       0x09B64C2BL,    0x7EB17CBDL,    0x0E7B82D07L,   0x90BF1D91L,
       0x1DB71064L,    0x6AB020F2L,    0x0F3B97148L,   0x84BE41DEL,
       0x1ADAD47DL,    0x6DDDE4EBL,    0x0F4D4B551L,   0x83D385C7L,
       0x136C9856L,    0x646BA8C0L,    0x0FD62F97AL,   0x8A65C9ECL,
       0x14015C4FL,    0x63066CD9L,    0x0FA0F3D63L,   0x8D080DF5L,
       0x3B6E20C8L,    0x4C69105EL,    0x0D56041E4L,   0x0A2677172L,
       0x3C03E4D1L,    0x4B04D447L,    0x0D20D85FDL,   0x0A50AB56BL,
       0x35B5A8FAL,    0x42B2986CL,    0x0DBBBC9D6L,   0x0ACBCF940L,
       0x32D86CE3L,    0x45DF5C75L,    0x0DCD60DCFL,   0x0ABD13D59L,
       0x26D930ACL,    0x51DE003AL,    0x0C8D75180L,   0x0BFD06116L,
       0x21B4F4B5L,    0x56B3C423L,    0x0CFBA9599L,   0x0B8BDA50FL,
       0x2802B89EL,    0x5F058808L,    0x0C60CD9B2L,   0x0B10BE924L,
       0x2F6F7C87L,    0x58684C11L,    0x0C1611DABL,   0x0B6662D3DL,

       0x76DC4190L,    0x01DB7106L,    0x98D220BCL,    0x0EFD5102AL,
       0x71B18589L,    0x06B6B51FL,    0x9FBFE4A5L,    0x0E8B8D433L,
       0x7807C9A2L,    0x0F00F934L,    0x9609A88EL,    0x0E10E9818L,
       0x7F6A0DBBL,    0x086D3D2DL,    0x91646C97L,    0x0E6635C01L,
       0x6B6B51F4L,    0x1C6C6162L,    0x856530D8L,    0x0F262004EL,
       0x6C0695EDL,    0x1B01A57BL,    0x8208F4C1L,    0x0F50FC457L,
       0x65B0D9C6L,    0x12B7E950L,    0x8BBEB8EAL,    0x0FCB9887CL,
       0x62DD1DDFL,    0x15DA2D49L,    0x8CD37CF3L,    0x0FBD44C65L,
```

【００５０】

【表２】

Sample C++ Source Code to Calculate CRC-32 （続き）

```
0x4DB26158L,  0x3AB551CEL,  0x0A3BC0074L,  0x0D4BB30E2L,
0x4ADFA541L,  0x3DD895D7L,  0x0A4D1C46DL,  0x0D3D6F4FBL,
0x4369E96AL,  0x346ED9FCL,  0x0AD6788461L,  0x0DA60B8D0L,
0x44042D73L,  0x33031DE5L,  0x0AA0A4C5FL,  0x0DD0D7CC9L,
0x5005713CL,  0x270241AAL,  0x0BE0B1010L,  0x0C90C2086L,
0x5768B525L,  0x206F85B3L,  0x0B966D409L,  0x0CE61E49FL,
0x5EDEF90EL,  0x29D9C998L,  0x0B0D09822L,  0x0C7D7A8B4L,
0x59B33D17L,  0x2EB40D81L,  0x0B7BD5C3BL,  0x0C0BA6CADL,

0x0EDB88320L,  0x9ABFB3B6L,  0x03B6E20CL,  0x74B1D29AL,
0x0EAD54739L,  0x9DD277AFL,  0x04DB2615L,  0x73DC1683L,
0x0E3630B12L,  0x94643B84L,  0x0D6D6A3EL  0x7A6A5AA8L,
0x0E40ECF0BL,  0x9309FF9DL,  0x0A00AE27L,  0x7D079EB1L,
0x0F00F9344L,  0x8708A3D2L,  0x1E01F268L,  0x6906C2FEL,
0x0F762575DL,  0x806567CBL,  0x196C3671L,  0x6E6B06E7L,
0x0FED41B76L,  0x89D32BE0L,  0x10DA7A5AL,  0x67DD4ACCL,
0x0F9B9DF6FL,  0x8EBEEFF9L,  0x17B7BE43L,  0x60B08ED5L,
0x0D6D6A3E8L,  0x0A1D1937EL,  0x38D8C2C4L,  0x4FDFF252L,
0x0D1BB67F1L,  0x0A6BC5767L,  0x3FB506DDL,  0x48B2364BL,
0x0D80D2BDAL,  0x0AF0A1B4CL,  0x36034AF6L,  0x41047A60L,
0x0DF60EFC3L,  0x0A867DF55L,  0x316E8EEFL,  0x4669BE79L,
0x0CB61B38CL,  0x0BC66831AL,  0x256FD2A0L,  0x5268E236L,
0x0CC0C7795L,  0x0BB0B47031,  0x220216B9L,  0x5505262FL,
0x0C5BA3BBEL,  0x0B2BD0B28L,  0x2BB45A92L,  0x5CB36A04L,
0x0C2D7FFA7L,  0x0B5D0CF31L,  0x2CD99E8BL,  0x5BDEAE1DL,

0x9B64C2B0L,  0x0EC63F226L,  0x756AA39CL,  0x026D930AL,
0x9C0906A9L,  0x0EB0E363FL,  0x72076785L,  0x05005713L,
0x95BF4A82L,  0x0E2B87A14L,  0x7BB12BAEL,  0x0CB61B38L,
0x92D28E9BL,  0x0E5D5BE0DL,  0x7CDCEFB7L  0x0BDBDF21L,
0x86D3D2D4L,  0x0F1D4E242L,  0x68DDB3F8L,  0x1FDA836EL,
0x81BE16CDL,  0x0F6B9265BL,  0x6FB077E1L,  0x18B74777L,
0x88085AE6L,  0x0FF0F6A70L,  0x66063BCAL,  0x11010B5CL,
0x8F659EFFL,  0x0F862AE69L,  0x616BFFD3L,  0x166CCF45L,
0x0A00AE278L,  0x0D70DD2EEL,  0x4E048354L,  0x3903B3C2L,
0x0A76726G1L,  0x0D06016F7L,  0x4969474DL,  0x3E6E77DBL,
0x0AED16A4AL,  0x0D9D65ADCL,  0x40DF0B66L,  0x37D83BF0L,
0x0A9BCAE53L,  0x0DEBB9EC5L,  0x47B2CF7FL,  0x30B5FFE9L,
0x0BDBDF21CL,  0x0CABAC28AL,  0x53B39330L,  0x24B4A3A6L,
0x0BAD03605L,  0x0CDD70693L,  0x54DE5729L,  0x23D967BFL,
0x0B3667A2EL,  0x0C4614AB8L,  0x5D681B02L,  0x2A6F2B94L,
0x0B40BBE37L,  0x0C30C8EA1L,  0x5A05DF1BL,  0x2D02EF8DL

};

UINT32 CRCFileBlock(UINT16 hFile, UINT32 lOffset, UINT32 lLength, UINT32 lSeed)
{
        // calculate CRC on file block with seed given
        // use 0xFFFFFFFFL for initial seed
        // returns 0 on success, returns lSeed on error
```

【００５１】

【表３】

Sample C++ Source Code to Calculate CRC-32 （続き）

```
    int ret;
    char buffer[COPYBUFFERLEN];
    UINT32 lRemainLength;
    UINT16 uBlockSize;
    UINT32 lSourceOff;
    UINT32 lCRC;
    UINT16 i, index;

    lCRC = lSeed;

    if(lLength > COPYBUFFERLEN)
        uBlockSize = COPYBUFFERLEN;
    else
        uBlockSize = (UINT16)lLength;

    lRemainLength = lLength;
    lSourceOff = lOffset;

    while(lRemainLength) {
        ret = ReadFileBlock(buffer, hFile, lSourceOff, uBlockSize);
        if(ret)
            return lSeed;

        for (i=0; i<uBlockSize; i++) {
            index = (UINT16)(lCRC ^ buffer[i]) & (UINT16)0x000000FFL;
            lCRC = ((lCRC >> 8) & 0x00FFFFFFL) ^ CRCTable[index];
        }
        lCRC = ~lCRC;

        lRemainLength -= uBlockSize;
        lSourceOff += uBlockSize;
        if(lRemainLength < uBlockSize)
            uBlockSize = (UINT16)lRemainLength;
    }

    return lCRC;
}

UINT32 CRCBlock(char* buffer, UINT16 nLength, UINT32 lSeed)
{
    // calculate CRC on file block with seed given
    // use 0xFFFFFFFFL for initial seed
    // returns 0 on success, returns lSeed on error (ignores error)

    UINT32 lCRC;
    UINT16 i, index;

    lCRC = lSeed;

    for (i=0; i<nLength; i++) {
        index = (UINT16)(lCRC ^ buffer[i]) & (UINT16)0x000000FFL;


        lCRC = ((lCRC >> 8) & 0x00FFFFFFL) ^ CRCTable[index];
    }
    lCRC = ~lCRC;
    return lCRC;
}
```

【００５２】

ＣＲＣ値をそれのみで使用することができるが、より高いレベルのセキュリティを本発明に組み込んで、画像の真実性を、ＣＲＣ値への数学的変換の追加によ

って保証することができる。上述したように、ＣＲＣ－３２を計算するための典型的なアルゴリズムはパブリックドメインにあり、したがって容易にアクセス可能である。この事実は、本明細書に提供された詳細と共に、いかなる者も、改変された画像のＣＲＣを再計算することができるようにし、「Ａｕｔｈｅｎｔｉｄａｔｅ」を偽造し、および画像が真実であり改変されていないと不正に確認することができる。本発明では、実際に計算された（画像または日付）ＣＲＣが、画像マーキングの前に新しい値に数学的に変換される。変換の機能要件は、いかなる入力値に対しても結果として生ずる値が一貫していること、および、結果として生ずる値が、一意の入力値に対して一意であることである。たとえば、変換を、入力のビット順序の順列、入力値と一貫した所定の「マジック」ナンバーとの排他的論理和、またはこれらの演算の組み合わせにすることができる。

【００５３】

実装された特定の変換技術は重要ではないが、本発明の実施において変換を実施するために使用された特定の技術が、プロバイダに内密に、すなわち「専有の変換技術」にすべきであり、この方法のいかなる開示または普及は、システムのセキュリティおよび有効性を損なう可能性があることを理解されたい。簡単な対比を与えると、専有の変換技術を保護することの失敗は、本質的に、ファイルをパスワードで保護し、次いでパスワードを配布することに等しいこととなる。

【００５４】

情報をデジタルファイル内のタグに記録することは、個々のデジタルファイルフォーマット、および、それらのフォーマットの構造の基準となる規格の知識を必要とする。これらの規格は、情報がファイルにおいてどのように、どの順序で、どの圧縮アルゴリズムを使用して格納されるかなどを指図する。大抵のデジタルファイルフォーマットは、画像データに加えて、デジタルファイルにおけるユーザデータの格納に対応するための規定を有する。本発明のＤｏｃＳＴＡＲファイル管理およびイメージングシステム実施形態は、既知のＴＩＦＦ（Ｔａｇｇｅｄ　Ｉｍａｇｅ　Ｆｉｌｅ）およびＪＰＥＧ（Ｊｏｉｎｔ　Ｐｈｏｔｏｇｒａｐｈｉｃ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）ファイルフォーマットを、（走査された）複調性およびカラー画像の格納のためにそれぞれ使用する。ＴＩＦＦおよびＪ

ＰＥＧ画像ファイルフォーマットの規格は、表示された画像に影響を与えない方法で、画像ファイル内部のユーザデータの包含を可能にする。容易に理解されるように、本発明は、ユーザにより定義されたデータをファイルに格納するための機構を有する他のファイルフォーマットに等しく適用可能であり、あるいは、ユーザにより定義されたデータによりマーキングされたファイルは、たとえば、ワードプロセッサ用文書、表計算、デジタル化されたオーディオまたはビデオまたは他のいかなるデジタル化されたファイル用の、補助的なファイルまたは分離したデータベースに格納することができる。

【００５５】

既知のＴＩＦＦフォーマットは、画像データを、圧縮された方法で、使用された圧縮方法、解像度、サイズ、色の数、タイトル、日付など画像についての情報（タグ）と共に格納することができるファイルフォーマットである。

【００５６】

書面にされた世界的な規格が、ＴＩＦＦファイルフォーマット、どのタグが存在しなければならないか、どのタグが任意選択か、および、特定のタグがどのように使用されるかを定義している。ＴＩＦＦ規格を維持している組織、Ａｄｏｂｅ　Ｃｏｒｐｏｒａｔｉｏｎは、タグをＴＩＦＦ画像内で使用するアプリケーションを開発する企業のためのカスタムタグ番号の要求を受け入れている。Ａｄｏｂｅは、一意の番号を個々の企業に割り当てて、ベンダの間の干渉を防止する。たとえば、本願の譲受人であるＢｉｔＷｉｓｅ　Ｄｅｓｉｇｎｓ，Ｉｎｃ．は、自身が所有するタグ番号を申し込み、割り当てられており、他のベンダも同様に、自身が所有する一意のタグ番号を割り当てられる。カスタムタグの使用が、カスタムデータブロックの格納を可能にする。ＴＩＦＦ仕様は、プログラムに、理解できない、およびベースライン仕様にないタグを無視するように命ずる。これにより、共通の画像ビューワが、カスタムタグを有する画像を閲覧し、表示し、印刷することができ、これは、画像ファイルがＴＩＦＦ仕様に適合するからである。

【００５７】

ＴＩＦＦ画像ファイルにおいて、以下のＴＩＦＦ画像タグが使用される。

Ｔａｇ＃　Ｕｓｅ

10Dh　Document Name

10Eh　Image Description

132h　Date Time

9244h　BitWise DocSTAR Custom Tag 1

custom data block contains proprietary information including:

Image CRC

Authentidate CRC

【００５８】

図５に示したものは、ＴＩＦＦ画像ファイル用の画像ＣＲＣの計算を示す例示的な流れ図である。ＴＩＦＦ画像ファイル用の画像ＣＲＣの計算は、所与の３２ビットのシード値を使用した、所与のデータのブロックにおけるＣＲＣ－３２の計算を要求する。初期シード値が－１に設定される（ステップ５００）。このルーチンが、ファイルのための画像ファイルディレクトリ（ＩＦＤ）に基づいたＴＩＦＦファイルのフォーマットで動作し、ＣＲＣ－３２を各ＩＦＤエントリおよびそれらの関連付けられたデータについて計算し（ステップ５０２）、先のＣＲＣ－３２の結果をシードとして次に（ステップ５１０）渡し、すべてのＩＦＤエントリを巡回するまで（ステップ５０６）行われる。

【００５９】

以下のタグおよびデータ領域を除く、すべてのタグおよびデータ領域が処理される（ステップ５０８）。

Ｔａｇ＃	Ｄｅｓｃｒｉｐｔｉｏｎ
０ｘ０１０ｄ	ＴＩＦＦＴＡＧ＿ＤＯＣＵＭＥＮＴＮＡＭＥ
０ｘ０１０ｅ	ＴＩＦＦＴＡＧ＿ＩＭＡＧＥＤＥＳＣＲＩＰＴＩＯＮ
０ｘ０１３２	ＴＩＦＦＴＡＧ＿ＤＡＴＥＴＩＭＥ
０ｘ９２４４	ＴＩＦＦＴＡＧ＿ＤＯＣＳＴＡＲＴＡＧ１

【００６０】

ファイルのすべてのＩＦＤエントリを処理した後（ステップ５０６）、専有の変換方法（上述した）が使用されて、結果として生じたＣＲＣ値を、一意かつ確

実な値ＣＲＣ′に変換する（ステップ５１２）。次に、変換された画像ＣＲＣ値であるＣＲＣ′は、画像ファイルに格納される（ステップ５１４）。

【００６１】

図６に示したものは、ＴＩＦＦ画像ファイル用の日付ＣＲＣの計算を示す例示的な流れ図である。ＴＩＦＦ画像ファイル用の日付ＣＲＣの計算が、所与の３２ビットのシード値を使用して、所与のデータのブロックにおけるＣＲＣ－３２を計算することができるルーチンを要求する。初期シード値は、画像ＣＲＣ値に設定する（ステップ６００）。このルーチンが、０ｘ０１３２　ＴＩＦＦＴＡＧ＿ＤＡＴＥＴＩＭＥタグを読み取る（ステップ６０２）。ＤＡＴＥＴＩＭＥタグが見つからず、読み取れなかった場合（ステップ６０４）、エラーが返され（ステップ６０５）、そうでない場合は、ＣＲＣ－３２は、ＤＡＴＥＴＩＭＥタグ内に含まれたデータについて計算される（ステップ６０６）。次に、結果としてのＣＲＣは、ＣＲＣ′に、専有の変換技術によって変換され（ステップ６０８）、画像ファイル内に格納される（ステップ６１０）。

【００６２】

Ｊｏｉｎｔ　Ｐｈｏｔｏｇｒａｐｈｉｃ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐが、同名のフォーマットを開発し、ＪＰＥＧおよびＪＰＧファイルフォーマット（時としてＪＦＩＦ－ＪＰＥＧファイル画像フォーマットとも呼ばれる）のための規格を維持している。このフォーマットは、写真画像の格納および伝送のために開発された。使用された圧縮技術は、理想的には、写真等の色変化の間の微妙な違いを格納することに適合される。

【００６３】

知られているように、ＪＰＧファイルは、画像情報および画像データの異なる要素を分離する「マーカ」と呼ばれる特殊な識別子により、文字のストリームとして解釈される。各マーカの厳密な意味は、ＪＰＧ規格が、特殊なまたは所有者独自の機能のために使用される１組のマーカを定義することを除いて、この考察には重要でない。これらのマーカは、「ＡＰＰｘ」と命名され、ただし、ｘは０と９の間の、両方を含む数字である。

【００６４】

本発明は、特殊なマーカおよびデータブロックをＪＰＧファイルに、それらが格納されるときに追加する。この実施形態では、「ＡＰＰ８」マーカが、このマーカがめったに他のメーカによって使用されないという簡単な理由のために使用される。このマーカが、以下を含む、様々な専有の情報を保持する。

Ａｕｔｈｅｎｔｉｄａｔｅ

画像ＣＲＣ

証明ＣＲＣ

【００６５】

図７に示したものは、ＪＰＥＧ画像ファイル用の画像ＣＲＣの計算を示す例示的な流れ図である。ＪＰＥＧ画像ファイル用のＣＲＣの計算が、所与の３２ビットのシード値を使用して、所与のデータのブロックにおけるＣＲＣ－３２を計算することができるルーチンを要求する。初期シード値が－１に設定される（ステップ７００）。画像ファイルデータが順次に読み取られ、ＡＰＰ８の位置が決定され、読み取られる（ステップ７０２）。ＡＰＰ８マーカが見つからず、読み取られなかった場合（ステップ７０４）、エラーが返される（ステップ７０５）。ＣＲＣ－３２が、ファイルにおけるすべてのデータについて、ファイルの最初から、ＡＰＰ８マーカを含まずに、ＡＰＰ８マーカまで計算される（ステップ７０６）。この計算の結果がシードとして使用されて、ＡＰＰ８マーカの後に続くファイルの残りにおいてＣＲＣ－３２が計算される（ステップ７０８）。結果として生じたＣＲＣは、ＣＲＣ′に専有の変換技術によって変換される（ステップ７１０）。次に、変換された画像ＣＲＣ′は、画像ファイル内に格納される（ステップ７１２）。

【００６６】

図８に示したものは、ＪＰＥＧ画像ファイル用の日付ＣＲＣの計算を示す例示的な流れ図である。ＪＰＥＧ画像ファイル用のＣＲＣの計算が、所与の３２ビットのシード値を使用して、所与のデータのブロックにおけるＣＲＣ－３２を計算することができるルーチンを要求する。初期シード値が画像ＣＲＣ値に設定される（ステップ８００）。ファイルが順次に読み取られ、ＡＰＰ８の位置が決定され、読み取られる（ステップ８０２）。ＡＰＰ８マーカが見つからず、読み取ら

れなかった場合（ステップ８０４）、エラーが返される（ステップ８０５）。ＣＲＣ－３２が、ＡＰＰ８データ領域またはブロック内の確実なデータ文字列について計算される（ステップ８０６）。結果として生じたＣＲＣは、ＣＲＣ′に専有の変換技術によって変換される（ステップ８０８）。変換された日付ＣＲＣ′は、画像ファイル内に格納される（ステップ８１０）。

【００６７】

本発明は、その特定の実施形態に関して例示され、記載された。しかし、上述した実施形態は、本発明の概念の例示的なものでしかなく、排他的な実施形態とすることを意図しないことを理解されたい。本発明の考察を容易にするため、デジタルイメージに走査される紙の文書の原本（たとえば、紙、写真など）が、本発明のＤｏｃＳＴＡＲ実施形態において仮定される。しかし、本発明が、いかなるデジタルファイルにも、そのソースまたはそれが生成される方法に関わらず、たとえば、デジタルカメラ、医療画像デバイス、文書処理または表計算アプリケーション、または他のソースから生ずるデジタルイメージに、等しく適用可能となることを、当業者は理解されたい。

【００６８】

本明細書に開示され、列挙された実施形態における変形形態を取りこむ代替実施形態を実施して、本発明の利点を達成することができる。

【００６９】

前述および多数の様々な変更、省略および追加を、本発明の精神および範囲から逸れることなく、当業者によって考案することができることを、さらに理解されたい。

【００７０】

したがって、本発明が、開示された実施形態に限定されず、特許請求の範囲にしたがって定義されるべきであることが意図される。

【図面の簡単な説明】

本発明の前述および他の特徴および利点は、添付の図面において例示されたように、以下のその例示的実施形態の詳細な説明に照らして、より明らかになるであろう。

【図１】

本発明のＤｏｃＳＴＡＲ実施形態のシステム実装を示す図である。

【図２】

本発明の一実施形態にかかるファイルマーキングを示す流れ図である。

【図３】

本発明の一実施形態にかかるファイルされマーキングされた画像のＣＲＣの検証を示す流れ図である。

【図４】

本発明の確実なクロックを設定するための一実施形態を示す流れ図である。

【図５】

本発明の一実施形態にかかるＴＩＦＦフォーマット画像の画像ＣＲＣの計算を示す流れ図である。

【図６】

本発明の一実施形態にかかるＴＩＦＦフォーマット画像の日付ＣＲＣの計算を示す流れ図である。

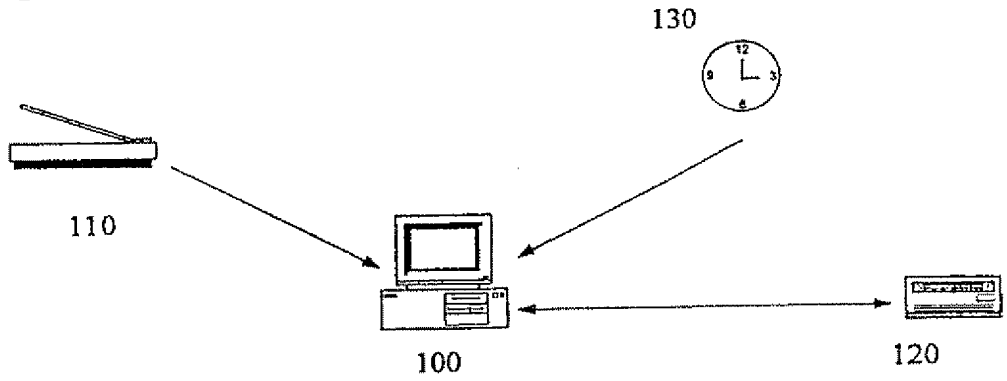
【図７】

本発明の一実施形態にかかるＪＰＥＧフォーマット画像の画像ＣＲＣの計算を示す流れ図である。

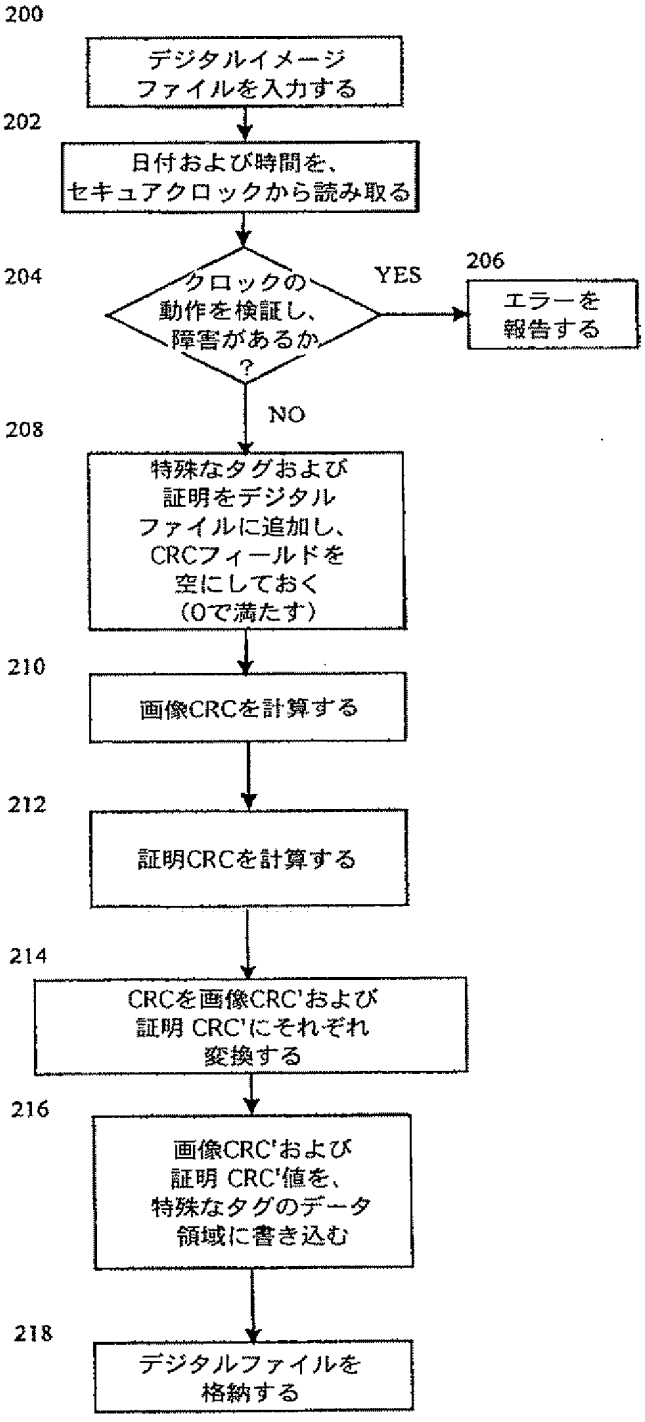
【図８】

本発明の一実施形態にかかるＪＰＥＧフォーマット画像の日付ＣＲＣの計算を示す流れ図である。

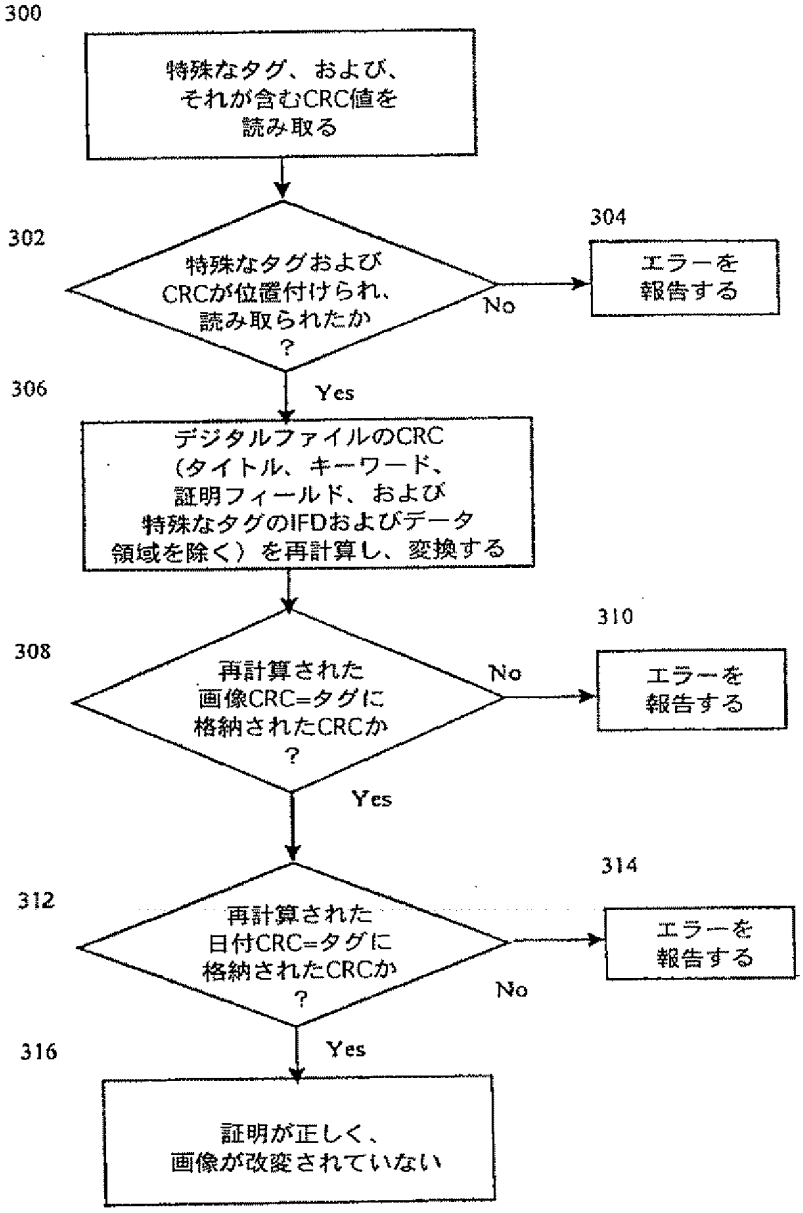
【図１】



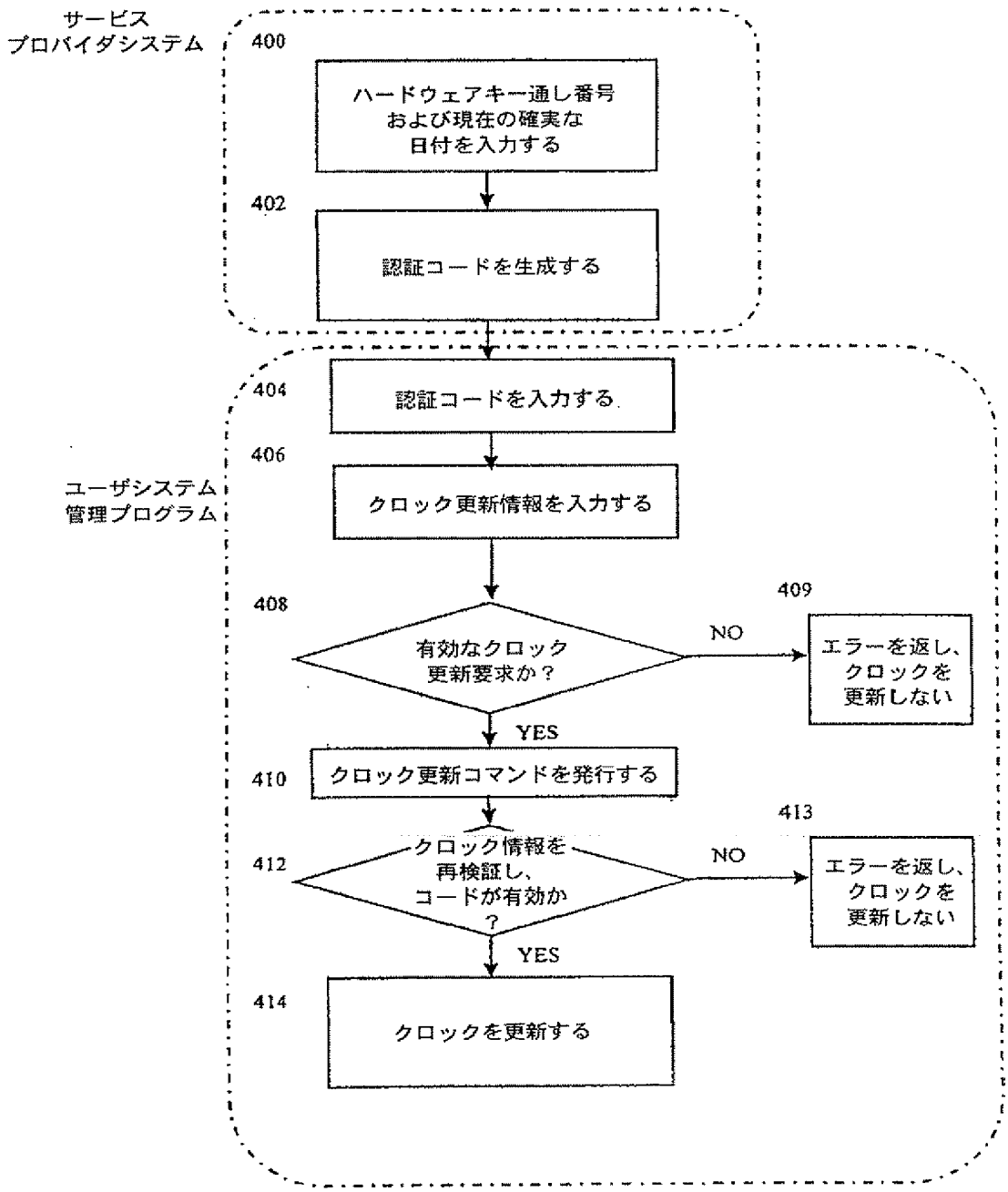
【図２】


200
デジタルイメージ
ファイルを入力する
202
日付および時間を、
セキュアクロックから読み取る
204
クロックの
動作を検証し、
障害があるか
？
YES
206
エラーを
報告する
NO
208
特殊なタグおよび
証明をデジタル
ファイルに追加し、
CRCフィールドを
空にしておく
（0で満たす）
210
画像CRCを計算する
212
証明CRCを計算する
214
CRCを画像CRC'および
証明 CRC'にそれぞれ
変換する
216
画像CRC'および
証明 CRC'値を、
特殊なタグのデータ
領域に書き込む
218
デジタルファイルを
格納する

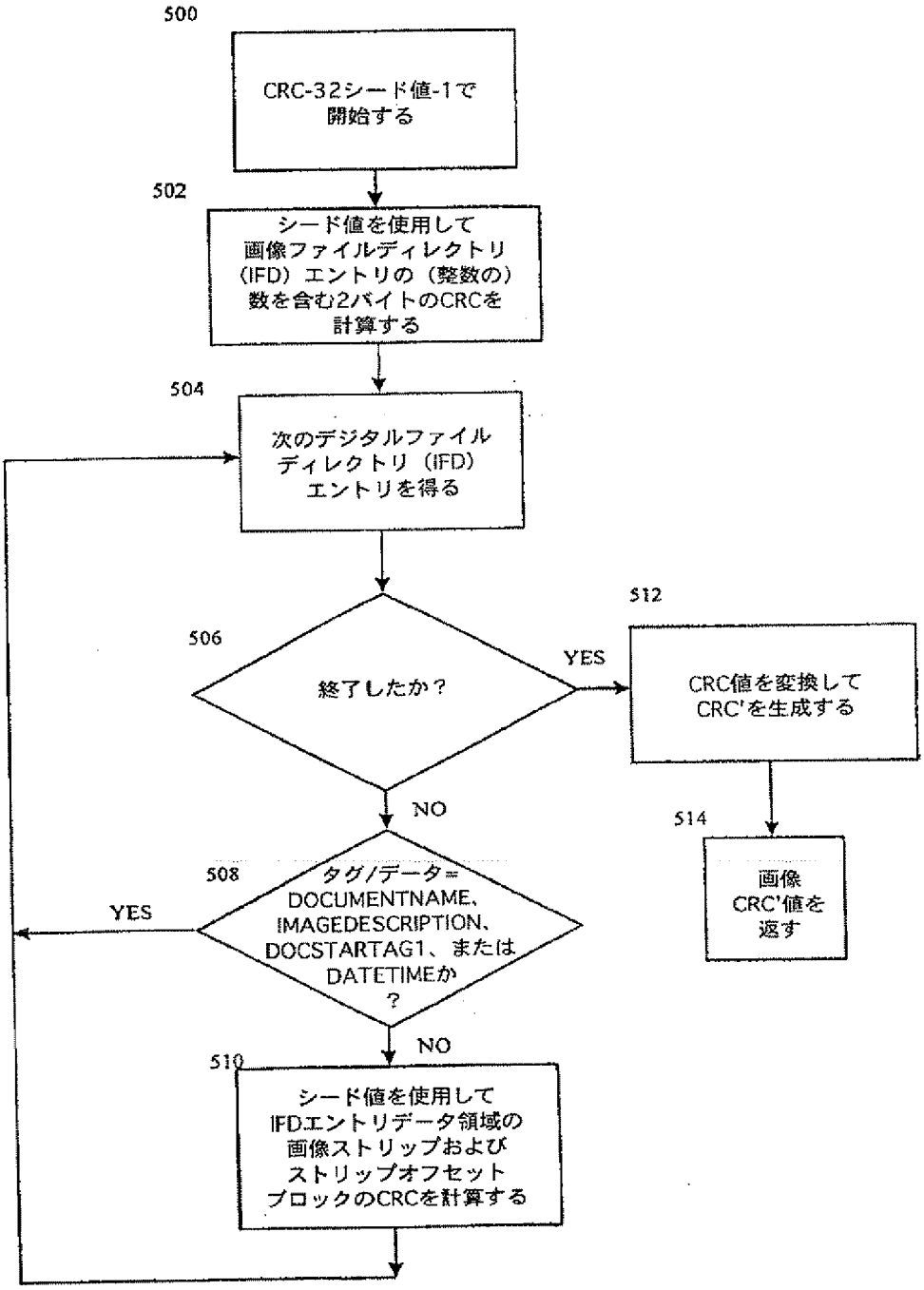
【図３】


300
特殊なタグ、および、
それが含むCRC値を
読み取る
302
特殊なタグおよび
CRCが位置付けられ、
読み取られたか
？
No
304
エラーを
報告する
Yes
306
デジタルファイルのCRC
（タイトル、キーワード、
証明フィールド、および
特殊なタグのIFDおよびデータ
領域を除く）を再計算し、変換する
308
再計算された
画像CRC=タグに
格納されたCRCか
？
No
310
エラーを
報告する
Yes
312
再計算された
日付CRC=タグに
格納されたCRCか
？
No
314
エラーを
報告する
Yes
316
証明が正しく、
画像が改変されていない

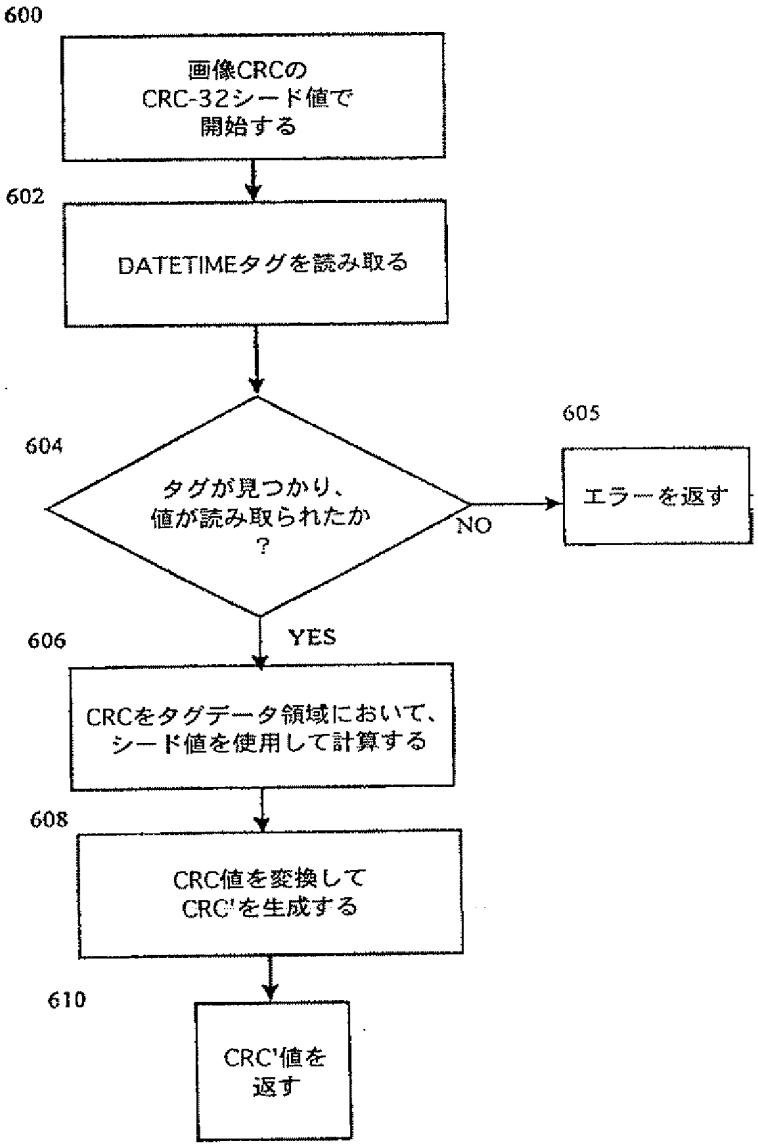
【図４】


サービス
プロバイダシステム
400
ハードウェアキー通し番号
および現在の確実な
日付を入力する
402
認証コードを生成する
ユーザシステム
管理プログラム
404
認証コードを入力する
406
クロック更新情報を入力する
408
有効なクロック
更新要求か？
NO
409
エラーを返し、
クロックを
更新しない
YES
410
クロック更新コマンドを発行する
412
クロック情報を
再検証し、
コードが有効か
？
NO
413
エラーを返し、
クロックを
更新しない
YES
414
クロックを更新する

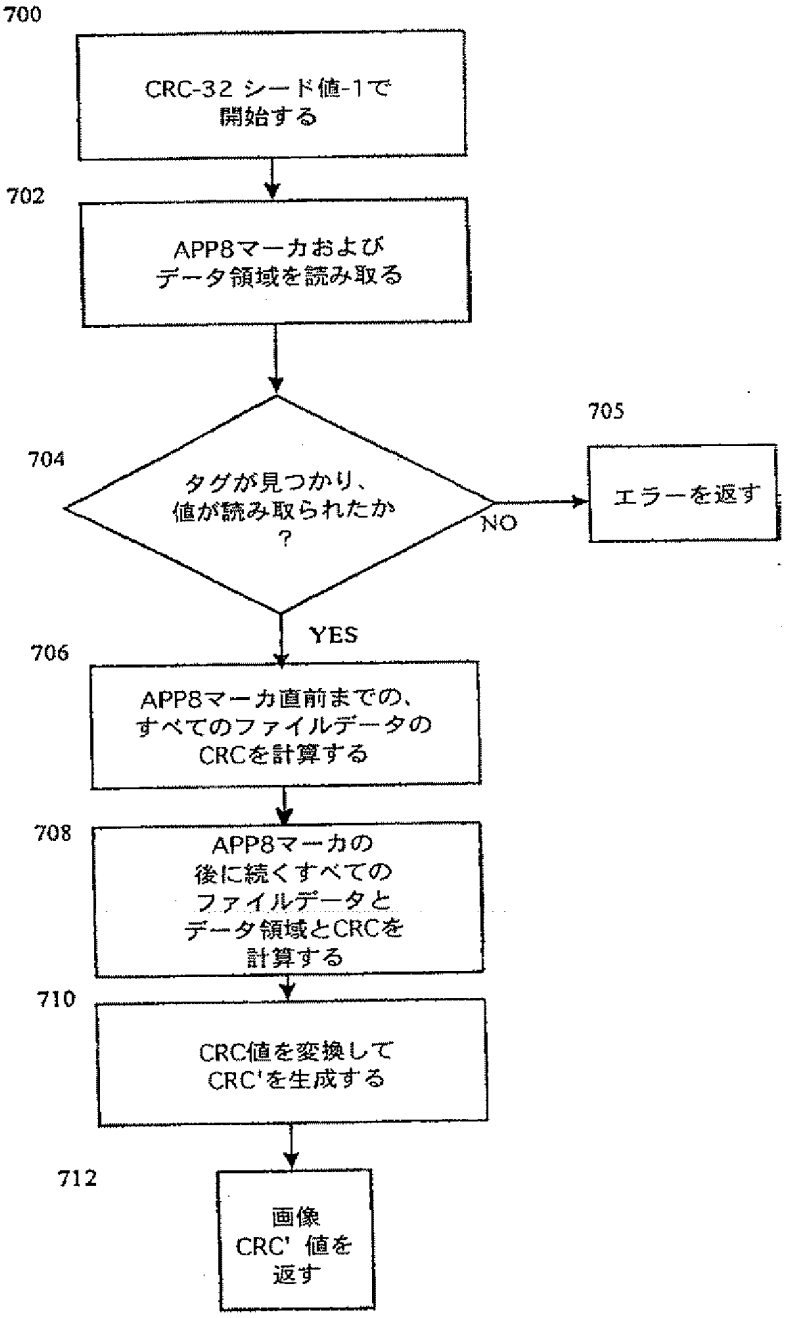
【図５】


500
CRC-32シード値-1で開始する
502
シード値を使用して画像ファイルディレクトリ（IFD）エントリの（整数の）数を含む2バイトのCRCを計算する
504
次のデジタルファイルディレクトリ（IFD）エントリを得る
506
終了したか？
YES
512
CRC値を変換してCRC'を生成する
514
画像CRC'値を返す
NO
508
タグ/データ＝DOCUMENTNAME、IMAGEDESCRIPTION、DOCSTARTAG1、またはDATETIMEか？
YES
NO
510
シード値を使用してIFDエントリデータ領域の画像ストリップおよびストリップオフセットブロックのCRCを計算する

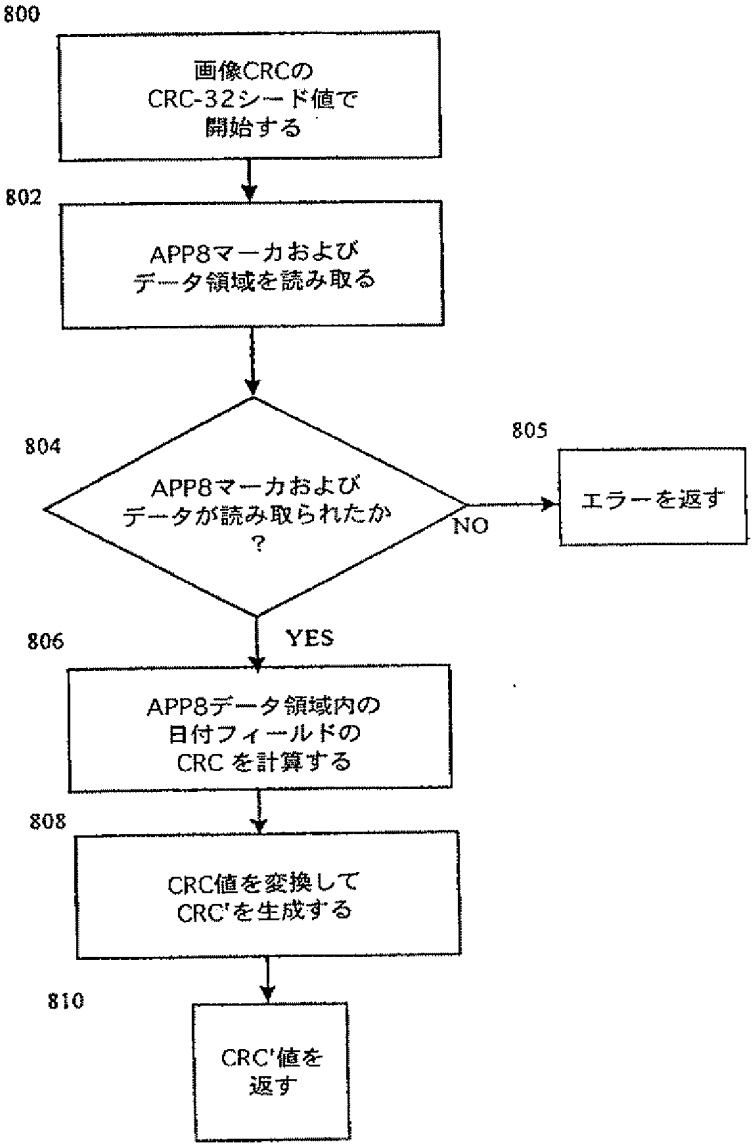
【図６】


600
画像CRCの
CRC-32シード値で
開始する
602
DATETIMEタグを読み取る
604
タグが見つかり、
値が読み取られたか
？
NO
605
エラーを返す
YES
606
CRCをタグデータ領域において、
シード値を使用して計算する
608
CRC値を変換して
CRC'を生成する
610
CRC'値を
返す

【図７】


700
CRC-32 シード値-1で
開始する
702
APP8マーカおよび
データ領域を読み取る
704
タグが見つかり、
値が読み取られたか
？
NO
705
エラーを返す
YES
706
APP8マーカ直前までの、
すべてのファイルデータの
CRCを計算する
708
APP8マーカの
後に続くすべての
ファイルデータと
データ領域とCRCを
計算する
710
CRC値を変換して
CRC'を生成する
712
画像
CRC' 値を
返す

【図８】


800
画像CRCの
CRC-32シード値で
開始する
802
APP8マーカおよび
データ領域を読み取る
804
APP8マーカおよび
データが読み取られたか
？
NO
805
エラーを返す
YES
806
APP8データ領域内の
日付フィールドの
CRC を計算する
808
CRC値を変換して
CRC'を生成する
810
CRC'値を
返す

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05098

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 9/08
US CL : 380/4, 54
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/4, 54, 3, 5; 707/104

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
NPL, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,875,249 A (MINTZER et al) 23 February 1999, see the abstract, Figure 1, column 1, lines 5-7, column 2, lines 33-38, column 3, lines 25-60	1-32
Y, P	US 5,949,879 A (BERSON et al) 07 September 1999, see the abstract, Figure 1.	1-32
Y	US 5,499,294 A (FRIEDMAN) 12 March 1996, see the abstract.	11, 23
Y	US 5,870,471 A (WOOTTON et al) 09 February 1999, see column 1, lines 39-50.	12, 24
Y, P	US 5,923,763 A (WALKER et al) 13 July 1999, see column 5, lines 34-45.	3, 4, 6, 8, 17, 18, 27, 28

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
20 MAY 2000	12 JUN 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer UYEN LE Telephone No. (703) 305-4134

Form PCT/ISA/210 (second sheet) (July 1998) *

フロントページの続き

(51)Int.Cl.7	識別記号	FI	テーマコード（参考）
H04N 1/40		H04N 1/40	Z

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

Fターム(参考) 5B001 AA04
5B017 AA02 BA07 CA16
5B050 BA10 EA10 GA07 GA08
5B082 AA13 EA10 GA11
5C077 LL14 NP05 PP23 PP78 PQ12
PQ22 TT10